DELL Technologies

Partners in Endpoint Resilience and Data Protection

In today's mobile business environment, endpoints are scattered across the globe. With easily disabled security controls, these devices – and the data they contain – are regularly lost, stolen, or operating without effective protection. With an estimated 70% of all breaches originating on endpoints, they are an organization's greatest source of risk.

Simultaneously, regulatory requirements continue to drive consumer data privacy concerns and, consequently, spur growth in the information security market. However, much of IT security spending is in vain due to broken controls caused by endpoint agent decay.

- 42% of endpoints are operating unprotected*
- 100% of security tools fail eventually*
- 5000+ common vulnerabilities and exposures (CVEs) released in the top 20 client applications**

* Absolute 2019 Endpoint Security Trends Report
** MITRE.ORG

Absolute Persistence®, The Path to Resilience

Absolute is the leader in endpoint security, providing unrivaled data and device protection to over 12,000 organizations globally. The cloud-based platform maintains a constant connection to devices, opening up unhindered visibility into an entire endpoint population.

Absolute Persistence technology is the only security agent embedded in the firmware of most Dell PCs, laptops, and tablets. Absolute can repair and restore any endpoint agent or control – on and off the corporate network. IT and security teams trust Absolute and Dell to protect data, prevent breaches, and maintain regulatory compliance.

Dell is a select OEM that can activate Absolute at the factory – so you can ensure your devices are protected from the very beginning of their lifecycle.

Learn more at DellEMC.com/endpointsecurity

Absolute enables you to see, understand, and control your entire endpoint population from a single pane of glass – no matter where the devices are located.

Asset Intelligence

Increase operational efficiency and reduce costs

Benefits:

- Eliminate blind spots and fragmentation across platforms
- Discover and reduce hardware and software waste
- Automate inventory and optimize device lifecycle management
- Save time data gathering for auditing and reporting

Capabilities:

- Maintain a self-healing connection to all endpoints – on or off the corporate network
- Implement quickly with a cloud-based console and no required infrastructure
- See and control your entire endpoint population from a single pane of glass
- Automate compliance checks and device usage reports

Visibility and Control

Persist security controls and configurations

Benefits:

- Harden gold image and enforce security controls
- Fortify encryption to reduce risk of exposure
- Maximize ROI of existing endpoint security technology
- Strengthen security posture and prevent compliance failures

Capabilities:

- Restore failing security agents with zero touch from IT
- Report on the health of security applications
- Assess your security posture with the security vitals dashboard
- Enforce configurations across your endpoint population at scale

Data and Device Security

Remotely detect and remediate vulnerable devices and at-risk data

Benefits:

- Protect lost or stolen devices from cyber threats
- Detect vulnerable devices and push fixes across your endpoints
- Prove compliance after an incident by validating that security controls were in place
- Prevent financial and reputational damage resulting from non-compliance

Capabilities:

- Freeze and delete data remotely on compromised devices
- Detect devices that leave an authorized area with geofencing
- Take any action on any device remotely on or off the network
- Receive custom alerts when regulated or confidential data is at-risk

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com to discuss how we can help improve your security posture.

Learn more at DellEMC.com/endpointsecurity